УДК 621.391

А.В. Снегуров, В.Х. Чакрян

Харьковский национальный университет радиоэлектроники, Харьков

ПОЛУМАРКОВСКАЯ МОДЕЛЬ ОЦЕНКИ КАЧЕСТВА УПРАВЛЕНИЯ ТРАФИКОМ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ С ПРЕДВЫЧИСЛЕНИЕМ ПУТЕЙ В УСЛОВИЯХ НАЛИЧИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается модель с использованием математического аппарата полумарковских процессов, которая позволяет оценивать эффективность управления трафиком в сетях с предварительным вычислением маршрутов на основании критериев качества обслуживания (QoS) и информационной безопасности.

Ключевые слова: *полумарковский процесс, информационная безопасность, динамическое резервирование маршрута, управление маршрутизацией, MPLS, QoS.*

Введение

В современных условиях выбор маршрута передачи информации определяется требованиями решения задач сбалансирования загрузки телекоммуникационных сетей (ТКС), задач обеспечения гарантий качества обслуживания – QoS (Quality of Service) и нформационной безопасности (ИБ). Сложность решения комплекса перечисленных задач обусловила появление концепции заблаговременной маршрутизации или маршрутизации с предвычислением путей PR (Precomputation Routing) [1]. В ходе PR на первом шаге заблаговременно рассчитывается множество путей между множеством пар узлов, а на втором шаге

осуществляется распределение трафиков пользователей по этим путям с выделением каждому из них необходимой пропускной способности с целью обеспечения заданных показателей качества обслуживания. Концепция PR заложена в т.н. модель "от управления" [1-4] при решении маршрутных задач в технологиях Tag Switching (Cisco Systems), IP Navigator (Ascend/Lucent) и ARIS (IBM), а также составляет основу стандарта MPLS (MultiProtocol Label Switching) путем присвоения каждому пути соответствующей метки или стека меток. Концепция PR в настоящее время получает все большое распространение вследствие своих преимуществ перед другими технологиями маршрутизации. Так, например, технология MPLS используется в магистральных сетях практически всех операторов и находит все большее распространение в территориальных локальных сетях.

Особенностью современных процессов маршрутизации является наличие большого количества угроз информационной безопасности, направленных на различные элементы системы маршрутизации. Так, например, согласно исследованию [5], в сети MPLS возможен неавторизованный доступ злоумышленников к трафику через взятие ими под контроль узлов сети. Возможны такие виды информационных атак, как компрометация устройств поставщика услуг, взлом станций управления сетью, атаки на транзитные устройства между провайдерами и т.д. Необходимо отметить, что обеспечение конфиденциальности информации эффективно решается с использованием шифрования трафика. Однако от данного способа защиты часто отказываются ради экономии и простоты администрирования виртуальной частной сети MPLS [5]. Нельзя в связи с этим исключать и «самую опасную уязвимость» любых современных информационных систем – человека, входящего в их систему управления. Кадровая политика провайдеров и влияние ее на информационную безопасность данных компаний и их клиентов является отдельным исследованием. Однако даже поверхностный анализ современного состояния этой темы показывает наличие огромного количества проблем.

Опасной для магистральной сети MPLS могут являться DDOS-атаки на клиентские сети, подключенные к такой сети. DDOS-атака приводит к росту интенсивности «вредоносного» трафика через маршрутизаторы магистральной сети, их перегрузке, и соответственно отказу или задержке в обслуживании «полезного» трафика. Сложность борьбы с такими атаками заключается в том, что для магистральной сети MPLS отличить «полезный» трафик от DDOS-трафика очень сложно.

В этих условиях актуальной задачей управления трафиком является выбор таких маршрутов передачи трафика, которые обеспечивали учет как требований качества обслуживания (QoS), так и требований информационной безопасности. Показателями качества маршрута в современных ТКС могут использоваться такие, как задержка информации, пропускная способность маршрута, загруженность и надежность каналов связи маршрута. Для учета информационной безопасности маршрута было предложено использовать такой показатель, как риск информационной безопасности узлов маршрута, зависящий от вероятности атаки на узлы сети злоумышленником и степень уязвимости системы защиты этих узлов от таких атак [6]. Использование данного показателя позволяет выбрать маршрут передачи пакетов с более низким риском нарушения конфиденциальности передаваемой информации. Однако учет требований при выборе маршрута к одним показателем может привести к недопустимому ухудшению качества работы системы, оцениваемой по другим показателям. Так, например, выбор более безопасного, с точки зрения обеспечения конфиденциальности информации, маршрута может не удовлетворять требованиям по времени задержки информации, что критично, например, для трафика сервисов реального времени (IP-телефония, IPTV, видео по запросу, аудио- и видео – конференции, VoIP и др.).

Поэтому важной задачей является разработка математической модели процесса передачи пакетов, позволяющей получить вероятностно-временные характеристики данного процесса при выборе маршрутов с различными особенностями их функционирования. Такими особенностями могут быть различная длительность маршрутов, различное количество маршрутизаторов на каждом из маршрутов и их эффективность работы (пропускная способность), различная интенсивность трафика на маршрутах, различные условия информационной безопасности трафика, передаваемого по разным маршрутам.

В статье для решения данной задачи предлагается полумарковская модель процесса передачи пакетов с учетом факта принятия решения в системе маршрутизации относительно маршрута. Использование полумарковской модели позволяет представить динамику процесса передачи пакетов в условиях информационных атак с учетом его вероятностно-временных характеристик.

Исследование полумарковских моделей для моделирования с процессов функционирования сложных технических систем в условиях конфликта (противодействия со стороны злоумышленников или противоборствующих организационно-технических систем) осуществлено в ряде работ [7-11]. Однако вопросы моделирования процесса функционирования системы маршрутизации в условиях наличия информационных атак с использованием данного математического аппарата в известной литературе исследованы не были.

Исследование процесса маршрутизации в условиях наличия угроз информационной безопасности, на наш взгляд, должна быть многоуровневой, при котором каждый из уровней определяется масштабом рассматриваемых процессов (табл. 1). Такой подход позволяет осуществить декомпозицию процесса маршрутизации конфликта высокого иерархического уровня на составляющие его более «простые» конфликты.

Таблица 1

Многоуровневый подход к моделированию
процесса функционирования системы маршрутизации в условиях наличия угроз ИБ

Уровень процесса	Суть процесса	Описание процесса
Первый уровень – функционирование системы маршрутизации в условиях угроз ИБ	Процесс маршрутизации	Передача пакетов, оценка и выбор маршрутов с учетом требований QoS и ИБ, оценка риска ИБ системы маршрутизации
Второй уровень – функционирование средств (подсистем) системы маршрутизации в условиях угроз ИБ	Процесс противоборства средств защиты маршрутизаторов (трафика) от соответствующих угроз ИБ	Реализация DDOS-атак и защита от них, вторжение в маршрутизаторы и защита маршрутизаторов существующими средствами (IDS, IPS, антивирусное программное обеспечение (ПО) и т.д.), криптографическая защита трафика и криптоанализ, действие средств радиоэлектронной борьбы по беспроводным ТКС и защита от них и т.д.
Третий уровень – функционирование частных процессов подсистем (средств) системы маршрутизации и средств информационного нападения	Частные процессы функционирования маршрутизаторов и средств информационного нападения	Обнаружение нападения, распознавание угрозы, принятие решения на применение методов защиты, передача информации об обнаружении угрозы и т.д.

На первом уровне детализации осуществляется анализ процессов маршрутизации, используемых протоколов и метрик оценки качества маршрута, учет стратегии и тактики действия системы маршрутизации и злоумышленников, выбор ими рефлексии различного уровня, использование злоумышленниками комплексной атаки через разные каналы воздействия и т.д. На данном этапе анализируются все уязвимые места в системе маршрутизации ТКС, все возможные средства и методы нападения, которые может выбрать злоумышленник.

На втором уровне детализации осуществляется рассмотрение процесса противоборства конкретных средств (подсистем) нападения и защиты, например, вредоносное ПО – антивирусные пакеты, средства проникновения в ТКС – система обнаружения вторжения и т.д. На данном уровне может возникнуть необходимость исследования возможности упреждения в действиях противоборствующей стороны, то есть – кто-кого успеет опередить в действиях.

Третий уровень детализации необходим для получения вероятностно-временных характеристик частных процессов конфликтного функционировании средств (подсистем) системы маршрутизации.

1. Полумарковская модель функционирования системы маршрутизации в условиях наличия угроз информационной безопасности

Рассмотрим в соответствии с первым уровнем модели (таблица 1) процесс передачи пакетов в системе с предвычислением путей PR для одного направления (i,j), где i – индекс входного LER (Label Edge Router) маршрутизатора, j – индекс выходного LER маршрутизатора. Считаем, что в направлении передачи пакетов (i,j) сети существует определенное количество маршрутов *K,* состоящее из различного количества LSR (Label Switching Router) маршрутизаторов. Составим граф состояний функционирования системы маршрутизации (рис.1).

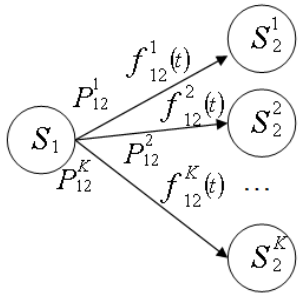

Рис. 1. Граф состояний работы
системы маршрутизации

В данной модели введены следующие обозначения: состояние S_1 – пакет поступил на входной LER маршрутизатор, решение на использование (изменение) маршрута принято, пакет начал передаваться по k–му маршруту, $k = [1, K]$; состояние S_2^k – пакеты дошли от входного LER маршрутизатора до выходного LER маршрутизатора по k–му маршруту; $f_{12}^k(t)$ - плотность распределения вероятности перехода из состояния S_1 в состояние S_2^k; $P_{12}^k(t)$ - вероятность выбора входным LER маршрутизатором

(системой маршрутизации) k-го маршрута передачи пакетов, $\sum_{k=1}^{K} P_{12}^{k} = 1$.

Данный граф описывается системой интегральных уравнений:

$$P_2^1(t) = P_{12}^1 \cdot \int_0^t f_{12}^1(t)dt \quad ,$$

$$P_2^2(t) = P_{12}^2 \cdot \int_0^t f_{12}^2(t)dt \, , \ldots, \; P_2^K(t) = P_{12}^K \cdot \int_0^t f_{12}^K(t)dt \, , \quad (1)$$

где $P_{12}^k(t)$ - вероятность доставки пакета от входного LER маршрутизатора до выходного LER маршрутизатора по k-му маршруту за время t, $k = [1, K]$.

Рассмотрим сущность вероятностей P_{12}^k. Выбор маршрутизатором (системой маршрутизации) k-го маршрута передачи пакетов зависит от используемого протокола маршрутизации. В настоящее время в сети MPLS применяются традиционные протоколы маршрутизации OSPF, IS-IS, BGP, каждый из которых использует свою систему оценки маршрутов передачи информации. Так маршруты в протоколе BGP характеризуются векторами расстояния до места назначения. В качестве метрики в протоколе OSPF используются «стоимость» маршрута, которая рассчитывается на основании пропускной способности каждого из его сегментов. Метрика, используемая в IS-IS, учитывает задержку информации, стоимость использования и надежность каналов связи маршрута.

В настоящее время проводятся исследования по включению в метрики маршрутизации показателей, учитывающих информационную безопасность маршрута передачи информации. Так, например, в [6] предложено в качестве функции, характеризующей весовой коэффициент любого k – го маршрута для направления передачи (i,j) с учетом требований QoS и информационной безопасности, выбрать соотношение:

$$D_k(\lambda_k) = \sum_{n=1}^{N_k} a^{R_n} \left(\frac{\lambda_n}{\mu_n - \lambda_n} + \tau_n^k \lambda_n \right), \quad (2)$$

где λ_n - информационный поток [1/c] в через n – узел k – го маршрута; μ_n - пропускная способность n-го узла [1/c] k-го маршрута; τ_n^k - задержка формирования и распространения пакетов [c] в n-м узле с учетом задержки в прилегающем к нему канале связи k – го маршрута, R_n, $R_n \in [0,1]$ - риск нарушения информационной безопасности n-го узла. Коэффициент a может изменяться в зависимости важности информации. Решение задачи маршрутизации для направления передачи (i, j) при этом сводится к нахождению целевой функции [12]:

$$D_{ij} = \min_{k \in (i,j)} \left(D_k(\lambda_k) \right), \quad k = \overline{1, K}, \quad (3)$$

Коэффициент R_n может определяться исходя из выражения:

$$R_n = 1 - \prod_{g=1}^{G} \left(1 - P_g^{угр} \cdot P_g^{уязв} \right), \quad (4)$$

где $P_g^{угр}$ - вероятность реализации g-й угрозы из множества G существующих угроз на n-й маршрутизатор; $P_g^{уязв}$ - вероятность уязвимости для g-й угрозы системы защиты n-го маршрутизатора.

Для оценки данных параметров необходимо составление матрицы сценариев нападения на систему маршрутизации с учетом различных уязвимостей современных маршрутизаторов. Оценка данных показателей опирается на модель второго уровня (таблица 1). При таком подходе к оценке качества маршрута, его выбор будет представлять собой вероятностную задачу, и зависеть от того, как в телекоммуникационной компании оценивают складывающуюся ситуацию с информационной безопасностью. Необходимо отметить, что злоумышленником может быть организована атака на процесс принятия решения системой маршрутизации при выборе маршрута с целью перенаправления трафика на неэффективные маршруты или маршруты со скомпрометированными маршрутизаторами.

Оценка показателей $f_{12}^k(t)$ предлагаемой модели позволяет учесть временные факторы функционирования системы маршрутизации. Временной интервал перехода системы из состояния S_1 в состояние S_2 для k-го маршрута можно выразить выражением:

$$t_{23}^k = \sum_{n=1}^{N_k} t_{распр}^n + \sum_{n=1}^{N_k} t_{обс}^n, \quad (4)$$

где $t_{распр}^n$ - время передачи пакетов по каналу связи, прилегающему к n-му промежуточному LSR маршрутизатору k-го маршрута; $t_{обс}^n$ - время обслуживания пакетов n-м LSR маршрутизаторе k-го маршрута; N_k – количество маршрутизаторов на k -м маршруте. Как правило, задержка пакетов на маршруте в условиях высокой интенсивности трафика определяется временем обслуживания пакетов в маршрутизаторах.

Время обслуживания пакетов маршрутизатором, складывается из времени ожидания пакета в очереди и времени обработки пакета маршрутизатором. Если время обработки пакета фиксировано и обычно невелико (от нескольких микросекунд до нескольких десятков микросекунд), то время ожидания пакета в очереди колеблется в очень

широких пределах и является, как правило, случайной величиной.

Если принять в качестве допущения, что маршрутизатор представляет собой одноканальную систему массового обслуживания (СМО) с ожиданием, входным потоком является пуассоновский поток, плотность вероятности распределения $t^n_{обс}$ обслуживания пакетов маршрутизатором будет описываться показательным законом.

$$f^n_{обс}(t) = \beta_{обс} \cdot e^{-\beta_{обс} t} , \qquad (5)$$

где $\beta_{обс} = \mu \cdot (1-\rho)$, интенсивность обслуживания пакета маршрутизатором с учетом времени обработки его маршрутизатором и времени ожидания пакета в очереди [13], $\rho = \lambda / \mu$; λ - интенсивность заявок на входе маршрутизатора; μ - интенсивность обработки заявок маршрутизатором.

Для определения плотности распределения вероятности перехода $f^k_{12}(t)$ необходимо провести свертку плотностей распределения $f^n_{обс}(t)$, $n = [1, N_k]$ для всех маршрутизаторов k-го маршрута, что является сложной задачей.

Если принять, что случайное время обслуживания пакетов маршрутизаторами сети есть независимые величины, то для маршрута, состоящего из нескольких маршрутизаторов, время задержки пакетов на маршруте определяется суммой времен обслуживания пакетов каждым маршрутизатором. Известно, что сумма α независимых одинаково распределённых экспоненциальных случайных величин имеет вид Гамма распределения, плотность распределения $f_{обс\sum}(t)$ которого описывается из выражения:

$$f_{обс\Sigma}(t) = \frac{\beta^{\alpha}_{обс}}{\Gamma(\alpha)} t^{\alpha-1} e^{-\beta_{обс} t}, \qquad (6)$$

где Г – функция Эйлера второго порядка.

Тогда в случае одинаковых условий функционирования маршрутизаторов на k –м маршруте в качестве показателя $f^k_{12}(t)$ принимается $f_{обс\sum}(t)$.

Недостатком данной модели является то, что интенсивность обслуживания пакетов маршрутизаторами маршрута должны быть приблизительно одинаковыми. В случае, если один или несколько маршрутизаторов маршрута работают в отличном от других маршрутизаторов режиме, например режиме перегрузки (вследствие их низких пропускных способностей или высокого трафика на входе), плотность вероятности распределения $f^k_{12}(t)$ можно найти как свертку плотности вероятности распределения $f_{обс\sum_н}(t)$ времени задержки пакетов в X_k маршрутизаторах, функционирующих в нормальных режимах, и плотности вероятности распределения $f^k_{обс\sum_п}(t)$ времени задержки пакетов в Y_k маршрутизаторах, функционирующих в режиме перегрузки, $N_k = X_k + Y_k$

$$f^k_{12}(t) = \int_{-\infty}^{+\infty} f^k_{обс\Sigma_н}(\tau) \cdot f^k_{обс\Sigma_п}(t-\tau) d\tau , \qquad (7)$$

Плотности вероятности $f^k_{обс\sum_н}(t)$ и $f^k_{обс\sum_п}(t)$ можно описать Гамма распределением с соответствующими параметрами $\beta^{\alpha}_{обс}$ и α.

2. Пример использования предлагаемой модели

Например, существует ТКС, в которой используются три маршрута передачи информации. Маршрут № 1 состоит из 11 LSR маршрутизаторов, маршрут № 2 - из 7 LSR маршрутизаторов, маршрут № 3 - из 5 LSR маршрутизаторов. Интенсивности обработки трафика для всех маршрутизаторов одинакова – 50 пакетов в секунду. Интенсивность трафика DDOS-атаки для маршрута № 3 - 5 пакетов в секунду. На маршруте № 1 и 2 DDOS-трафик отсутствует. Суммарный трафик составляет: для маршрута № 1 – 44 пакета в секунду, для маршрута № 2 – 44 пакета в секунду, для маршрута № 3 – 49 пакетов в секунду. Входной LER маршрутизатор должен выбрать один маршрут для передачи пакетов.

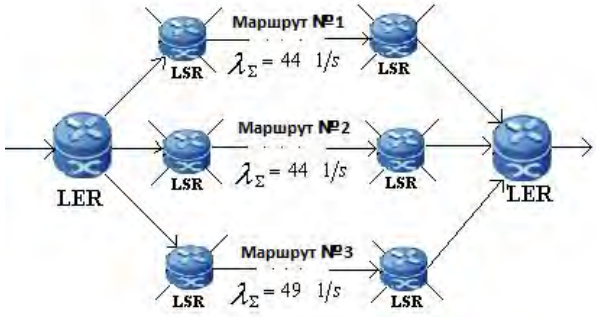

Рис. 2. Фрагмент ТКС для примера использования предлагаемой модели

Плотности распределения вероятности перехода системы маршрутизации из состояния S_1 в состояния S^k_2, а также зависимости вероятности своевременной доставки пакетов от времени для данных маршрутов и указанных условий их функционирования представлена на рис. 3 и 4. Из рисунков видно, что анализируемые маршруты имеют разную эффективность доставки пакетов. Если, например, оценить вероятность доставки пакетов за 2 секунды, то данный показатель составит: для маршрута № 1 – 0,4, для маршрута № 2 – 0,95, для маршрута № 3 – 0,05. При этом маршрут № 3 является самым коротким, но вследствие перегрузки самым неэффективным.

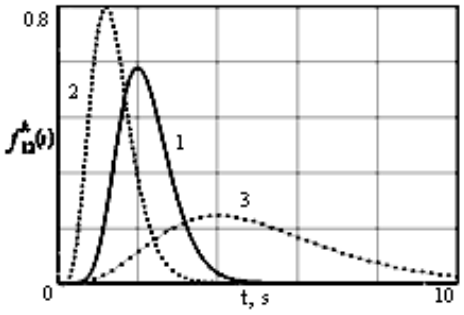

Рис. 3. Плотность распределения вероятности передачи трафика на выходной LER маршрутизатор по разным маршрутам

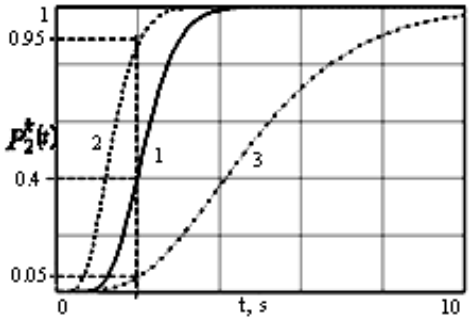

Рис. 4. Вероятность доставки пакетов на выходной LER маршрутизатор по разным маршрутам в зависимости от времени

Выводы

Предлагаемая модель, основанная на математическом аппарате полумарковских процессов, позволяет подойти к оценке качества работы системы маршрутизации как с позиций задач обеспечения гарантий качества обслуживания QoS, так и обеспечения информационной безопасности. Недостатками данной модели является необходимость обоснованного определения плотностей распределения вероятностей переходов системы (процессов) из состояния в состояние, сложность многократной свертки данных плотностей распределения вероятности при описании последовательно по времени проходящих процессов. Дальнейшие исследования в данном направлении будут посвящены созданию моделей функционирования ТКС для различных современных телекоммуникационных технологий с анализом и усовершенствованием механизмов обеспечения их информационной безопасности.

Список литературы

1. Лемешко А.В. Вероятностно-временная модель QoS-маршрутизации с предвычислением путей в условиях отказов элементов телекоммуникационной сети / А.В. Лемешко // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2005. – Вып. 142. – С. 11-20.

2. Younis O. Constraint-based routing in the internet: basic principles and recent research / O. Younis, S. Fahmy // IEEE Communication Society Surveys & Tutorials. – 2003. – Vol.5, №3. – P. 42-56.

3. Orda A., Sprintson A. QoS Routing: The Precomputation Perspective / A. Orda, A. Sprintson // Proc. IEEE INFOCOM. New York, 2000. – Vol. 3. – P. 283-291.

4. Cui Y. Precomputation for multi-constrained QoS routing in high-speed networks / Y. Cui, K. Xu, J. Wu // Proc. IEEE INFOCOM. – San Francisco, 2003. – Vol. 1. – P. 1305-1315.

5. Рей Э. Технология MPLS и сценарии нападения [Электронный ресурс] / Энно Рей, Петер Фирс // Журнал сетевых решений LAN, – 2006 – № 09, – Режим доступа: http://www.osp.ru/lan/2006/09/3169702/.

6. Snigurov A. Approach to the formation of routing metrics based of information security risk / A. Snigurov, V. Chakran // CADSM'2013, 19-23 February, 2013, Polyana-Svalyava (Zakarpattya), UKRAINE.

7. Сухоруков Ю.С. Динамика ситуационных конфликтов /В книге Дружинин В.В., Конторов Д.С., Конторов М.Д. - Введение в теорию конфликта // М. Радио и связь, 1989. – С. 280 – 285.

8. Методические основы формирования модели конфликта [Текст] / Козирацкий, Ю. Л. [и др.] // Телекоммуникации. - 2011. - N 4. - С. 2-7.

9. Модель процесса возникновения и протекания конфликта информационных средств разных видов / Козирацкий, Ю. Л. [и др.] // Радиосистемы. - 2011. - N 27. - С. 6-11.

10. Будников С.А. Полумарковская модель сложного конфликта радиоэлектронных систем [Текст] / С.А. Будников // V Межд. конф. «Методы и средства управления технологическими процесами», Саранск, 19 – 21 ноября 2009 года. Режим доступа: – http://fetmag.mrsu.ru/2009-2/.

11. Обоснование характеристик конфликтно-обусловленных переходов в полумарковских вероятностных моделях [Текст] / Подлужный В.И. [и др.] // Радиотехника. - 2006. - N 9. - С. 84-87.

12. Gallager R.G. A minimum delay routing algorithm using distributed computation / R.G. Gallager // IEEE Trans. on com.. – 1975. – Vol. 25, №1. – P.73-85.

13. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок. – М.: Машиностроение, 1979. – 432 с.

Поступила в редколлегию 15.10.2013

Рецензент: д-р техн. наук, проф. А.В. Лемешко, Харьковский национальный университет радиоэлектроники, Харьков.

НАПІВМАРКІВСЬКА МОДЕЛЬ ОЦІНКИ ЯКОСТІ УПРАВЛІННЯ ТРАФІКОМ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З ПОПЕРЕДНІМ ОБЧИСЛЕННЯМ ШЛЯХІВ В УМОВАХ НАЯВНОСТІ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А.В. Снігуров, В.Х. Чакрян

В даній статті пропонується модель з використанням математичного апарату напівмарківських процесів, що дозволяє оцінити ефективність управління трафіком в мережах з попереднім обчисленням маршрутів на основі критеріїв якості обслуговування (QoS) та інформаційної безпеки.

Ключові слова: *напівмарківський процес, інформаційна безпека, динамічне резервування маршруту, управління маршрутизацією, MPLS, QoS.*

SEMI-MARKOV MODEL OF TRAFFIC CONTROL QUALITY ASSURANCE IN TELECOMMUNICATION NETWORKS WITH ROUTES PRECALCULATION CONSIDERING RISKS OF INFORMATION SECURITY

A.V. Snigurov, V.K. Chakrian

In this paper it is proposed the model with usage of mathematical technique of semi-Markov processes that let evaluate the efficiency of traffic control in networks with routes precalculation based on quality of service (QoS) and information security.

Keywords: *Semi-Markov process, informative safety, dynamic backuping of route, management routing, MPLS, QoS.*